

b. Any change under this criteria requires a change in the "Retrievability" caption of the system notice.

c. If the records are no longer retrieved by name or personal identifier, cancel the system notice.

4. A change in the purpose for which the information in the system is used.

a. The new purpose must not be compatible with the existing purposes for which the system is maintained or a use that would not reasonably be expected to be an alteration.

b. If the use is compatible and reasonably expected, there is no change in purpose and no alteration occurs.

c. Any change under this criterion requires a change in the "Purpose(s)" caption and may require a change in the "Authority for maintenance of the system" caption.

5. Changes that alter the computer environment (such as changes to equipment configuration, software, or procedures) so as to create the potential for greater or easier access.

a. Increasing the number of offices with direct access is an alteration.

b. Software releases, such as operating systems and system utilities that provide for easier access are considered alterations.

c. The addition of an on-line capability to a previously batch-oriented system is an alteration.

d. The addition of peripheral devices such as tape devices, disk devices, card readers, printers, and similar devices to an existing ADP system constitute an amendment if system security is preserved.

e. Changes to existing equipment configuration with on-line capability need not be considered alterations to the system if:

(1) The change does not alter the present security posture.

(2) The addition of terminals does not extend the capacity of the current operating system and existing security is preserved.

f. The connecting of two or more formerly independent automated systems or networks together creating a potential for greater access is an alteration.

g. Any change under this caption requires a change to the "Storage" caption element of the systems notice.

C. Reports of new and altered systems. Submit a report of a new or altered system to DLA Support Services (DSS-CA) before collecting information and for using a new system or altering an existing system.

D. *Time restrictions on the operation of a new or altered system.* 1. All time periods begin from the date OSD signs the transmittal letters on the reports to OMB and Congress. The specific time limits are:

a. Sixty days must elapse before collection forms or formal instructions pertaining to the system may be issued.

b. Sixty days must elapse before the system may become operational.

c. Sixty days must elapse before any public issuance of a Request for Proposal or Invitation to Bid for a new ADP or telecommunication system.

NOTE: Requests for delegation of procurement authority may be submitted to the General Services Administration during the 60 days' waiting period, but these will include language that the Privacy Act reporting criteria have been reviewed and that a system report is required for such procurement.

d. Normally 30 days must elapse before publication in the FEDERAL REGISTER of the notice of a new or altered system and the preamble to the FEDERAL REGISTER notice must reflect the date the transmittal letters to OMB and Congress were signed by OSD.

2. Do not operate a system of records until the waiting periods have expired.

E. *Outside review of new and altered systems reports.* If no objections are received within 30 days of a submission to the President of the Senate, Speaker of the House of Representatives, and the Director, OMB, of a new or altered system report, it is presumed that the new or altered systems have been approved as submitted.

F. *Waiver of time restrictions.* 1. The OMB may authorize a Federal agency to begin operation of a system of records before the expiration of time limits described above. When seeking such a waiver, include in the letter of transmittal to DLA Support Services (CA) an explanation why a delay of 60 days in establishing the system of records would not be in the public interest. The transmittal must include:

a. How the public interest will be affected adversely if the established time limits are followed.

b. Why earlier notice was not provided.

2. Under no circumstances will the routine uses for a new or altered system be implemented before 30 days have elapsed after publication of the system notice containing the routine uses in the FEDERAL REGISTER. This period cannot be waived.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Re-designated and amended at 56 FR 57803, Nov. 14, 1991; 66 FR 41782, Aug. 9, 2001]

APPENDIX C TO PART 323—INSTRUCTIONS FOR PREPARATION OF REPORTS TO NEW OR ALTERED SYSTEMS

The report on a new or altered system will consist of a transmittal letter, a narrative statement, and include supporting documentation.

A. *Transmittal Letter.* The transmittal letter shall include any request for waivers. The narrative statement will be attached.

B. *Narrative Statement.* The narrative statement is typed in double space on standard bond paper. The statement includes:

Pt. 323, App. D

32 CFR Ch. I (7-1-08 Edition)

1. *System identification and name.* This caption sets forth the identification and name of the system.

2. *Responsible official.* The name, title, address, and telephone number of the official responsible for the report and to whom inquiries and comments about the report may be directed by Congress, the Office of Management and Budget, or Defense Privacy Office.

3. *Purpose of the system or nature of the change proposed.* Describe the purpose of the new system. For an altered system, describe the nature of the change being proposed.

4. *Authority for the system.* See enclosure 1 of this part.

5. *Number of individuals.* The approximate number of individuals about whom records are to be maintained.

6. *Information on First Amendment activities.* Describe any information to be kept on the exercise of the individual's First Amendment rights and the basis for maintaining it.

7. *Measures to ensure information accuracy.* If the system is to be used to make determinations about the rights, benefits, or entitlements of individuals, describe the measures being established to ensure the accuracy, currency, relevance, and completeness of the information used for these purposes.

8. *Other measures to ensure system security.* Describe the steps taken to minimize the risk of unauthorized access to the system. A more detailed assessment of security risks and specific administrative, technical, and physical safeguards will be available for review upon request.

9. *Relationship to state and local government activities.* Describe the relationship of the system to state or local government activities that are the sources, recipients, or users of the information in the system.

C. *Supporting Documentation.* Item 10 of the narrative is captioned *Supporting Documents*. A positive statement for this caption is essential for those enclosures that are not required to be enclosed. For example, "No changes to the existing DLA procedural or exemption rules (32 CFR part 323) are required for this proposed system." List in numerical sequence only those enclosures that are actually furnished. The following are typical enclosures that may be required:

1. For a new system, an advance copy of the system notice which is proposed for publication; for an altered system an advance copy of the notice reflecting the specific changes proposed.

2. An advance copy of any proposed exemption rule if the new or altered system is to be exempted. If there is no exemption, so state in the narrative.

3. Any other supporting documentation that may be pertinent or helpful in understanding the need for the system or clarifying its intended use. While not required,

such documentation, when available, is helpful in evaluating the new or altered system.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Redesignated and amended at 56 FR 57803, Nov. 14, 1991]

APPENDIX D TO PART 323—WORD PROCESSING CENTER (WPC) SAFEGUARDS

A. *Minimum Standards of Protection.* All personal data processed using word processing equipment will be afforded the standards of protection required by this regulation. The special considerations discussed in this enclosure are primarily for Word Processing Centers (WPCs) operating independent of the customer's function. However, managers of word processing systems are encouraged to consider and adopt, when appropriate, the special considerations described. WPCs that are not independent of a customer's function are not required to prepare formal written risk assessments.

B. *WPC Information Flow.* In analyzing procedures required to safeguard adequately personal information in a WPC, the basic elements of WPC information flow and control must be considered. These are: Information receipt, information processing, information return, information storage and filing. WPCs do not control information acquisition or its ultimate use by the customers and, therefore, these are not addressed.

C. *Safeguarding Information During Receipt.* 1. The word processing manager will establish procedures:

a. That require each customer who requests that information subject to this DLAR be processed to identify specifically that information to the WPC personnel. This may be done by:

(1) Providing a check-off type entry on the WPC work requests.

(2) Requiring that the WPC work requests be stamped with a special legend, or that a special notation be made on the work requests.

(3) Predesignating specifically a class of documents as coming within the provisions of this DLAR (such as, all officer effectiveness reports, all recall rosters, and all medical protocols).

(4) Using a special cover sheet both to alert the WPC personnel as to the type information, and to protect the document during transmittal.

(5) Requiring an oral warning on all dictation.

(6) Any other procedures that ensure the WPC personnel are alerted to the fact that personal data subject to this DLAR is to be processed.

b. To ensure that the operators or other WPC personnel who receive data for processing not identified as being under the provisions of this DLAR, but that appear to be